Lecture Notes in Computer Science 7079

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Emmanuel Prouff (Ed.)

Smart Card Research and Advanced Applications

10th IFIP WG 8.8/11.2 International Conference
CARDIS 2011
Leuven, Belgium, September 14-16, 2011
Revised Selected Papers

Volume Editor

Emmanuel Prouff
Oberthur Technologies
71-73 rue des Hautes Pâtures
92726 Nanterre Cedex, France
E-mail: e.prouff@oberthur.com

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-27256-1 e-ISBN 978-3-642-27257-8
DOI 10.1007/978-3-642-27257-8
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011943215

CR Subject Classification (1998): E.3, C.2, K.6.5, D.4.6, C.3, D.2

LNCS Sublibrary: SL 4 – Security and Cryptology

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

These proceedings contain the papers selected for CARDIS 2011, the 10th IFIP Conference on Smart Card Research and Advanced Applications hosted by the Katholieke Universiteit of Leuven, Belgium. Since 1994, CARDIS has been the foremost international conference dedicated to the security of smart cards and embedded systems. Initially biennial, the conference became annual in 2010 to take into account the very fast evolution of the smart card technology.

Security of smart cards is today an established and dynamic research area. Since 1994, CARDIS offers a privileged environment where the scientific community can congregate, present new ideas and discuss recent developments with both an academic and industrial focus. It covers a wide range of topics including hardware design, operating systems, systems modelling, cryptography and systems security. This year, the Program Committee of CARDIS refereed 45 submitted papers. Each paper was reviewed by at least 3 referees and the committee selected 20 papers to be presented at the conference. Two invited talks completed the technical program. The first one was given by Helena Handschuh, Chief Technology Officer at Intrinsic-ID, and the second one, by Olivier Ly, Associate Professor at LaBRI, University of Bordeaux.

There are many volunteers who offered time and energy to put together the symposium and who deserve our acknowledgement. I first would like to thank all the members of the Program Committee and the external reviewers for their hard work in evaluating and discussing the submissions. I am also very grateful to Vincent Rijmen, the General Chair of CARDIS 2011, and his team for the local conference management. I am particularly grateful to the CARDIS Steering Committee for allowing me to serve at such a recognized conference. Especially, I would like to say a big thank you to Jean-Jacques Quisquater for all the energy and hard work he put into the organization of this event.

Last, but certainly not least, my thanks go to all the authors who submitted papers and all the attendees. I hope you will find the proceedings stimulating.

September 2011 Emmanuel Prouff

Organization

CARDIS 2011 was organized by the Katholieke Universiteit of Leuven, Belgium.

Executive Commitee

Conference General Chair

Vincent Rijmen	Katholieke Universiteit Leuven, Belgium

Program Committee Chair

Emmanuel Prouff	Oberthur Technologies

Publicity Chair

Jean-Jacques Quisquater	Université Catholique de Louvain, Belgium

Program Committee

Gildas Avoine	UCL Crypto Group, Belgium
Guido Bertoni	STMicroelectronics, Italy
Sébastien Canard	Orange Labs, France
Odile Derouet	Samsung, Korea
Josep Domingo Ferrer	Rovari i Virgili University, Catalonia
Hermann Drexler	Giesecke And Devrient, Germany
Benoit Feix	Inside Secure, France
Benedikt Gierlichs	K.U. Leuven, ESAT-COSIC, Belgium
Sylvain Guilley	GET/ENST, CNRS/LTCI, France
Kimmo Järvinen	Helsinki University of Technology, Finland
Jean-Louis Lanet	University of Limoges, France
Thanh-Ha Le	Morpho, France
Stefan Mangard	Infineon Technologies, Germany
Konstantinos Markantonakis	University of London, UK
Amir Moradi	Ruhr University Bochum, Germany
Ventzi Nikov	NXP, Belgium
Elisabeth Oswald	University of Bristol, UK
Axel Poschman	Nanyang Technological University, Singapore
Emmanuel Prouff	Oberthur Technologies, France
Matthieu Rivain	CryptoExperts, France
Jörn-Marc Schmidt	IAIK TU Graz, Austria

Sergei Skorobogatov	University of Cambridge, UK
François-Xavier Standaert	UCL Crypto Group, Belgium
Pim Tuyls	Intrinsic-ID, The Netherlands
David Vigilant	Gemalto, France

Referees

J. Balasch	J. Daemen	L. Hoffmann
S. Riou	R. Trujillo-Rasua	M. Hutter
A. Barenghi	E. De Mulder	M. Kasper
M. Roussellet	G. Van Assche	C.H. Kim
E. Beck	F. De Santis	S.-K. Kim
S. Salgado	V. Van Der Leest	F. Koeune
A. Berzati	E. Dottax	S. Kutzner
G. Schrijen	N. Veyrat-Charvillon	M. Le Guin
S. Bhasin	I. Eichhorn	M. Medwed
M. Seysen	K. Villegas	F. Melzani
B. Brumley	J. Fan	O. Mischke
J. Soria-Comas	O. Farràs	D. Oswald
C. Capel	W. Fischer	P. Paillier
A. Séré	G. Gagnerot	T. Plos
C. Clavier	B.M. Gammel	B. Qin
P. Teuwen	J. Großschädl	M. Quisquater
I. Coisel	V. Guérin	F. Regazzoni
C. Troncoso	S. Hajian	

Sponsoring Institution

Oberthur Technologies

Table of Contents

Smart Cards System Security

Invasive Attacks

New Algorithms and Protocols

Implementations and Hardware Security 1

Implementations and Hardware Security 2

Non-invasive Attacks

Java Card Security